NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 106988
21 May 2019

EMMA BEST
MUCKROCK NEWS
DEPT MR 73100
411A HIGHLAND AVE
SOMERVILLE MA 02144-2516

Dear Ms. Best:

This responds to your Freedom of Information Act (FOIA) request of 15 May 2019, which was received in the National Security Agency (NSA) FOIA office on 15 May 2019, for "Records, reports, emails, memos and other documents mentioning or relating to the Network Crack Program Hacker Group, a Chinese hacker group based out of Zigong in Sichuan Province." Your request has been assigned Case Number 106988. There are no assessable fees for this request. Your request has been processed under the FOIA.

NSA collects and provides intelligence derived from foreign communications to policymakers, military commanders, and law enforcement officials. We do this to help these individuals protect the security of the United States, its allies, and their citizens from threats such as terrorism, weapons of mass destruction, foreign espionage, international organized crime, and other hostile activities. What we are authorized to do, and how we do it, is described in Executive Order 12333. Information about how NSA conducts signals intelligence activities is available on the websites of NSA (www.nsa.gov) and the Office of the Director of National Intelligence (www.dni.gov).

To the extent that you are seeking non-intelligence records, the document you requested is enclosed. Certain information, however, has been deleted from the enclosure.

This Agency is authorized by statute to protect certain information concerning its activities, as well as the names of its employees. Such information is exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable in this case is Section 6, Public Law 86-36 (50 U.S. Code 3605). We have determined that such information exists in this record, and we have excised it accordingly.

In addition, certain information was withheld because it was not responsive to your request.

To the extent that you are seeking intelligence records, we have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

  NSA FOIA/PA Appeal Authority (P132)
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932

  The facsimile number is 443-479-3612.
  The appropriate email address to submit an appeal is FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

FOIA Case: 106988

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877-684-6448
(Fax) 202-741-5769

Sincerely,

Michael Shields
for

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

[redacted]

(b)(3)-P.L. 86-36

From: [redacted]
Sent: Friday, September 21, 2012 3:06 AM
To: Inglis John C NSA-D USA CIV
Subject: (U) Daily Pointers Daily Notification

Non - Responsive

[redacted]

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

(U) New IE exploit variant distributes PlugX malware.

(U) Researchers from security vendor AlienVault have identified a variant of a recently discovered Internet Explorer exploit that is used to infect targeted computers with the PlugX remote access Trojan (RAT) program. The newly discovered exploit variant targets the same unpatched vulnerability in IE 6, 7, 8 and 9 as the original exploit, but uses slightly different code and has a different payload, AlienVault Labs manager Jaime Blasco said Tuesday in a blog post. The first exploit was found over the weekend on a known malicious server by security researcher Eric Romang and distributed the Poison Ivy RAT. The second exploit version discovered by AlienVault researchers was found on a different server and installs a much newer RAT program called PlugX. However, file modification dates seen on both servers suggest that both versions of the exploit have been in use since at least 14 September. AlienVault researchers have been tracking attacks that use the PlugX RAT since earlier this year. Based on file debug paths found inside the malware, they believe that the relatively new RAT was developed by a Chinese hacker known as WHG, who had previous ties with the Network Crack Program Hacker (NCPH), a well known Chinese hacker group. AlienVault researchers have also identified two additional websites that served the new IE exploit in the past, but no payload could be obtained from them, Blasco said. One was a defense news site from India and the other was probably a fake version of the 2nd International LED professional Symposium website, he said. "It seems the guys behind this 0day were targeting specific industries," Blasco said. The server where the original IE exploit was found also stored an exploit for an unpatched Java vulnerability last month. That Java exploit was used in attacks attributed by security researchers to a Chinese hacker group dubbed "Nitro." Microsoft already released a security advisory about the new IE vulnerability and recommended temporary mitigation solutions while it works on a patch. (IDG News Service 19Sep12)

Non - Responsive

Non - Responsive